UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/009,840	05/01/2002	Olivier Lenoir	0501-1052	1234

466 7590 07/09/2008

YOUNG & THOMPSON
209 Madison Street
Suite 500
ALEXANDRIA, VA 22314

EXAMINER	
DINH, MINH	
ART UNIT	PAPER NUMBER
2132	

NOTIFICATION DATE	DELIVERY MODE
07/09/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

embon@young-thompson.com

Office Action Summary	Application No.	Applicant(s)	
	10/009,840	LENOIR ET AL.	
	Examiner	Art Unit	
	MINH DINH	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 March 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2 and 4-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2 and 4-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This office action is in response to the amendment filed 03/05/2008. Claims 1, 4, 9-11 have been amended; claim 3 has been canceled.

Response to Arguments

2. Applicant's arguments filed 03/05/08 have been fully considered but they are not persuasive. Applicant argues that Guthrie (6,161,185) does not disclose that the authentication password is directly built by a human user knowing a key because the authentication password is generated by a SADB calculator (page 13).

Guthrie discloses that a user provides a key and a random password as inputs to password calculator software run on the user's computer to generate an authentication password (fig. 5, elements 114 and 110; col. 5, lines 18-20; col. 7, lines 27-37). Since it is the user, not anyone else, that directly operates the password calculator to build the authentication password, Guthrie's user directly builds the authentication password. If Applicant had intended for the authentication password to be mentally generated/built by the user without utilizing any software and/or hardware means, it is suggested that the claims be amended to clearly recite such a limitation provided that it is supported by the original disclosure.

Claim Rejections - 35 USC § 112

3. Claims 1-12 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter

which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

The amended claim 1 recites the new limitation "a sequence of building an authentication password (MPAUT) from said voice message (MPA) directly by said user by applying a key known from said user to the voice message". Applicant states (see Response, page 10) that the new feature "the authentication password (MPAUT) is directly built by the user" disclosed in page 4, lines 17-19 of the application, that means that the user is directly doing an intellectual step and does not require any special identification computer device to built the authentication password (MPAUT); this characteristic is supported by the application, for example page 8, lines 17-20.

Lines 17-19 of the specification only disclose that the invention does not required any special identification computer device other than a conventional mobile phone and the user's client computer. The language in the passage does not exclude a scenario where the user utilizes the processing power of the user's client computer or the mobile phone to generate an authentication password.

Lines 17-20 of the specification disclose "a voice message intended to be processed directly by the aforesaid user for generating an authentication password", which can be understood by one of ordinary skill in the art as that the user must first listen to the message in order to get the information indicated in the voice message and then uses the information for generating an authentication password. However, the language in the passage does not disclose building an authentication password

(MPAUT) from said voice message (MPA) directly by said user by applying a key known from said user to the voice message.

Therefore, the limitation is considered new matter.

Claim Rejections - 35 USC § 103

4. Claims 1-2, 4-6, 9-10 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ratayczak (US 6,259,909 B1) in view of Guthrie et al. (US 6,161,185).

- Regarding claims 1, 4, 9-10 and 12, Ratayczak discloses a process of securing the access to a data processing server from a client site through at least a first communication network, i.e., Internet, this server comprising means for handling a protocol of authenticating a client site user, i.e., a person, comprising:

a sequence of receiving and processing identification data of a client site user (figures 5-6, step S51; col. 6, lines 59-67),

a sequence of transmitting a message indicating a random password from the server site to a client site user owned communication equipment through a second communication network (i.e., a telephone and a fixed telephone network), said communication equipment having a call number searched from an authentication data base (figures 5-6, step S52; col. 7, lines 1-5, 36-47; col. 4, lines 12-25),

a sequence of building an authentication password from the random password directly by the user (i.e., the user enters the value of the random password displayed by the phone into the user's computer) (figures 5-6, step S53; col. 7, lines 6-12)

a sequence of transmitting said authentication password to said server site through said first communication network (figures 5-6, step S54; col. 7, lines 13-18).

Ratayczak does not disclose that the message is a voice message. However, it is well known in the art that not all landline telephones have a display. Therefore, it would have been obvious to modify Ratayczak's method such that the message is a voice message since there would be no other option for landline telephones that do not have a display.

Ratayczak does not disclose that the authentication password is built by applying a key known from the user to the random password. Guthrie discloses method for generating authentication password, i.e., a one-time password, used in level two of a two-level authentication protocol wherein the authentication password used in level two is built, at the client user side, directly by the user by applying a key shared by the user and the server (i.e., the user's SADB password) to a random password (i.e., a random challenge) using password calculator software (figure 5; col. 7, lines 27-37). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate Guthrie's method for generating the one-time password into Ratayczak's method so that the server could determine that the authentication password was generated by an entity that knew the shared secret key.

- Regarding claim 2, Ratayczak discloses the securing process according to claim 1, characterized in that it comprises steps of:

requesting identification data (ID, MPC) from the client site through the first communication network (column 6 lines 59-64);

processing the aforesaid data (ID, MPC) and searching an authentication database for a client user owned communication equipment call number (this is inherent in column 7 lines 1-5 and 36-44 in that the server must know the call number of the mobile device from the HLR described in column 4 lines 12-24);

calling the aforesaid communication equipment through at least a second communication network (column 7 lines 1-5 and 36-44);

after establishing a communication with the aforesaid mobile communication equipment, generating a random or pseudo random password (MPA) (column 7 lines 36-40);

sending a voice message comprising the aforesaid random password through the second communication network (column 7 lines 1-5, see also above);

requesting the user provide, from the client site through the first communication network an authentication password (7 lines 13-15) derived from the aforesaid random or pseudo random password; and

authenticating the aforesaid authentication password (column 7 lines 13-15).

- Regarding claim 5, Ratayczak further discloses that the identification data requested from the client consists of a couple [identification code/client password] (column 6 lines 59-64).
- Regarding claims 6, Guthrie further discloses that the one-time password is valid only for a short period of time (col. 2, lines 48-53). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ratayczak's method such that the one-time password is valid only for a short period of time, as

taught by Guthrie. The motivation for doing so would have been to foil a malicious user's attempt at "hammering" the authentication system with response attempting to stumble upon a correct password and gain access (col. 2, lines 48-53).

5. Claims 7-8 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ratayczak in view of Guthrie as applied to claims 1 and 9 above, and further in view of Kelly (5,636,280).

- Regarding claims 7 and 11, Ratayczak discloses the securing process according to claim 1, characterized in that it comprises on the server side the steps of:

requesting identification data (ID, MPC) from the client site through the first communication network (column 6 lines 59-64);

processing the aforesaid data (ID, MPC) and searching an authentication database for a client user owned mobile communication equipment call number (this is inherent in column 7 lines 1-5 and 36-44 in that the server must know the call number of the mobile device from the HLR described in column 4 lines 12-24);

calling the aforesaid communication equipment through at least a second communication network (column 7 lines 1-5 and 36-44);

in case the communication is established with the aforesaid mobile communication equipment, send a voice message requesting the user to send an encryption key (Column 4 lines 55-62, wherein the codeword can be used as an encryption key as stated in column 7 lines 59-62);

receiving and recognizing the encryption key transmitted by the client by means of the mobile equipment keyboard (column 4 lines 59-65),

Ratayczak does not disclose using the key by the client user side to encrypt an authentication password transmitted to the server and using the key by the server to decrypt the encrypted password for authentication. Kelly discloses an authentication method wherein the user's password is encrypted using a key shared with a server prior to being transmitted to the server, and that the server uses the shared key to decrypt the encrypted password for authentication (fig. 4, steps 126, 128 and 130). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ratayczak's method to use the key by the client user side to encrypt an authentication password transmitted to the server and use the key by the server to decrypt the encrypted password for authentication, as taught by Guthrie. The motivation for doing so would have been to protect the password when it was transmitted from the client to the server.

- Regarding claim 8, Ratayczak does not disclose that the code word, which is used as the encryption key, is valid only a short period of time. Guthrie further discloses that a one-time password is valid only for a short period of time (col. 2, lines 48-53). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Ratayczak and Kelly such that the code word is valid only for a short period of time, as taught by Guthrie. The motivation for doing so would have been to foil a malicious user's attempt at "hammering" the authentication system with response attempting to stumble upon a correct password and gain access (col. 2, lines 48-53).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 6,078,908 to Schmitz

7. **THIS ACTION IS MADE FINAL**. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MINH DINH whose telephone number is (571)272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/M. D./
Examiner, Art Unit 2132

06/04/08

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132